(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11120679 A**

(43) Date of publication of application: **30 . 04 . 99**

(51) Int. Cl **G11B 19/04**
G11B 23/30

(21) Application number: **10162552**

(22) Date of filing: **10 . 06 . 98**

(30) Priority: **10 . 06 . 97 US 97 871953**

(71) Applicant: **SONY CORP OF AMERICA SONY CORP**

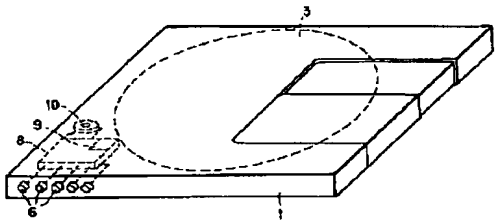
(72) Inventor: **GEORGE S BIRDMESSER**

(54) **DATA RECORDER AND DATA READING METHOD**

(57) Abstract:

PROBLEM TO BE SOLVED: To restrict the user's access or the number of accesses to data recorded on a read-only recording medium by confirming the identification information in the manner of reading out the identification requesting data from the recording medium or the access data from a storage means, and interrupting the access to the recording medium till the identification signal is received.

SOLUTION: The identification information is read out from an optical disk 3 by a computer when the existence is decided by an access controller 8. Next, the polling is made so that the number N of accesses to the optical disk 3 stored in a memory 9 is decided by the controller 8. Next, the maximum accessible number M is read out from the optical disk 3 by the computer. Then, these N and M are compared to decide whether the further accessing right exists for the user or not. At this time, when N is smaller than M, the further accessing right exists, and the remaining accessible number is informed to the user by the computer.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－120679

(43)公開日　平成11年(1999)４月30日

(51)Int.Cl.[6]	識別記号	Ｆ Ｉ	
Ｇ１１Ｂ　19/04	５０１	Ｇ１１Ｂ　19/04	５０１Ｈ
23/30		23/30	Ｚ

審査請求　有　　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－162552

(22)出願日　平成10年(1998)６月10日

(31)優先権主張番号　０８／８７１９５３

(32)優先日　1997年６月10日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　398062725
ソニー　コーポレーション　オブ　アメリカ
アメリカ合衆国　ニュージャージー州　07656　パーク　リッジ　ソニー　ドライブ　1

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　ジョージ　エス　バードメッサー
アメリカ合衆国　ニュージャージー州　07675　ウッドクリフ　レイク　ミルロード　エクステンション　12

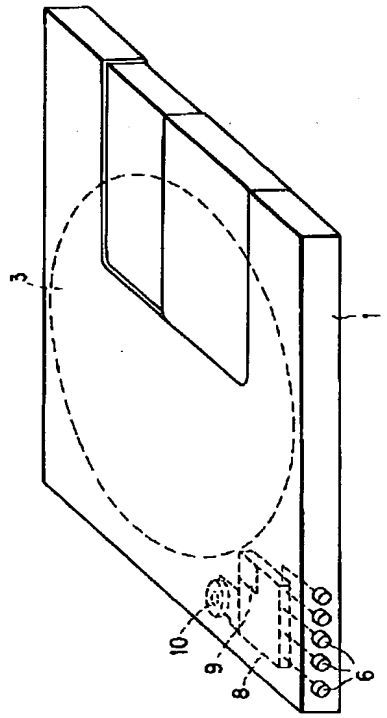
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　データ記録装置及びデータ読出方法

(57)【要約】

【課題】　光ディスクなどの書込不可の記録媒体に記録されたデータへのアクセス又はアクセス回数を制限するデータ記録装置及びデータ読出方法を提供する。

【解決手段】　カートリッジに収納された記録媒体から認証情報を読み出し、カートリッジに配設されたメモリからアクセス情報を読み出し、認証情報とアクセス情報を比較し、アクセスが認証されているときにのみ記録媒体からプログラム情報を読み出し、アクセスが認証されていないときはカートリッジを排出する。



1

【特許請求の範囲】

【請求項１】　筐体と、

上記筐体内に収納された、プログラムデータ及び認証要求データを記録する記録媒体と、

上記筐体内に配設され、アクセスデータを記憶する記憶手段と、

上記記憶手段に接続され、該記憶手段と認証情報を送受するためのインターフェース手段と、

上記記録媒体から上記認証要求データを読み出し、上記記憶手段から上記アクセスデータを読み出して認証情報を確認し、認証信号を生成する認証確認手段と、

上記認証信号を受信するまで上記記録媒体へのアクセスを阻止するアクセス阻止手段とを備えるデータ記録装置。

【請求項２】　上記記憶手段は、メモリと、メモリコントローラと、電源とを備えていることを特徴とする請求項１記載のデータ記録装置。

【請求項３】　上記記憶手段は消去可能プログラマブル読出専用メモリであることを特徴とする請求項１記載のデータ記録装置。

【請求項４】　上記インターフェイス手段は、上記筐体の側面に配設された接点を備えることを特徴とする請求項１記載のデータ記録装置。

【請求項５】　上記認証要求データは、上記記録媒体にアクセス可能な回数を示し、上記アクセスデータは、上記記録媒体に実際にアクセスがあった回数を示し、

上記記録媒体にアクセスがあったときに上記アクセスがあった回数を増加させるアクセス回数増加手段をさらに備えることを特徴とする請求項１記載のデータ記録装置。

【請求項６】　上記認証要求データは、上記記録媒体に与えられた固有の第１のシリアル番号であり、上記アクセスデータは、第２のシリアル番号であり、上記認証確認手段は、上記第１のシリアル番号と上記第２シリアル番号が一致するときに上記認証信号を生成することを特徴とする請求項１記載のデータ記録装置。

【請求項７】　上記記録媒体は光ディスクであることを特徴とする請求項１記載のデータ記録装置。

【請求項８】　上記記録媒体は、コンパクトディスク読出専用メモリであることを特徴とする請求項１記載のデータ記録装置。

【請求項９】　上記記録媒体は、デジタルビデオディスクであることを特徴とする請求項１記載のデータ記録装置。

【請求項１０】　上記記憶手段は、上記筐体に取り外し可能に装着された該筐体の一部を形成するモジュール内に配設されることを特徴とする請求項１記載のデータ記録装置。

【請求項１１】　データ記録装置に収納された記録媒体から認証情報を読み出すステップと、

2

上記データ記録装置に配設されたメモリからアクセス情報を読み出すステップと、

上記認証情報と上記アクセス情報を比較するステップと、

アクセスが認証されているときに上記記録媒体からプログラム情報を読み出すステップとを有するデータ読出方法。

【請求項１２】　上記メモリが上記データ記録装置内に存在するか否かを判定するステップと、

上記記録媒体に記録された認証情報がメモリの存在を必要とするか否かを判定するステップと、

上記認証情報がメモリの存在を必要とし、上記メモリが存在しないときには、上記記録媒体からのプログラム情報の読み出しを阻止するステップとを有することを特徴とする請求項１１記載のデータ読出方法。

【請求項１３】　パスコードを受信するステップと、

上記パスコードが正しいか否かを判定するステップと、

パスコードが正しいときに上記メモリのアクセス情報をリセットするステップとを有することを特徴とする請求項１１記載のデータ読出方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ記録装置及びデータ読出方法に関し、例えば、デジタルデータを記録した記録媒体を収納するカートリッジと、ユーザがデータにアクセスした回数を監視するプログラミング可能な監視装置により、ユーザが所定回数以上データにアクセスできないようにするデータ記録装置及びデータ読出方法に関する。

【０００２】

【従来の技術】データ記録の高密度化が進み、リムーバブルカートリッジに収納された記録媒体に、大量のデータを記録することができるようになった。ユーザは記録媒体が収納されたカートリッジを購入し、或いは借りて、何回でもその記録媒体に記録されたデータにアクセスすることができる。カートリッジの製造業者は、出荷したカートリッジ内の記録媒体に記録されたデータ又はプログラムを複数のユーザがコピーして使用する畏れがあるため、それによる損益を補償すべくカートリッジの出荷額を高めに設定することがある。ここで、認証を与えたユーザに対し、カートリッジ内の記録媒体にアクセスする回数を制限することができれば、製造業者は、カートリッジをより安く、多くのユーザに提供することができる。

【０００３】さらに、製造業者は、ユーザに対して所定数のワークステーションにソフトウェアをインストールすることを許諾するいわゆる機器設置契約（site license）を行う場合がある。このとき、契約されたソフトウェアを記録する記録媒体を収納した従来型のカートリッジをユーザに引き渡すと、認証されていないワークステ

ーションにそのソフトウェアがインストールされてしまう畏れがある。

【０００４】リムーバブルカートリッジ内の記録媒体に記録されたデータ又はプログラムへのユーザのアクセスを制限する手法として、例えば磁気ディスク等の記録媒体自体にアクセス情報を記録し、これによりユーザのアクセスを制限するような手法が知られている。ここでは、ユーザのコンピュータが記録媒体に認証情報を書き込み及び更新するようになっている。

【０００５】このような手法は、書き込みができない記録媒体には、用いることができない。例えば、光ディスクに対しては、ユーザが所有するような機器では書き込みを行えない。このような光ディスクには、例えばコンパクトディスク読出専用メモリ（ＣＤ－ＲＯＭ）やデジタルビデオディスク（ＤＶＤ）等がある。

【０００６】記録媒体自体にデータを記録することなく、記録媒体を収納したカートリッジの使用を監視する装置も提案されている。例えば、ラング他（Lang et al.）により１９９７年１月６日に出願された米国特許出願番号０８／７７８，６０４には、記録媒体用のカートリッジ内の機械的なポインタが開示されている。このポインタは、互換性を有するディスクドライブ内で、アクチュエータにより駆動される。カートリッジ内の記録媒体にデータが記録され、或いは消去されると、ポインタが移動し、記録媒体上の書込可能エリアの残量を示す。このポインタを用いて、記録媒体上の書込可能エリアの残量を示す代わりに、アクセス回数を示すこともできるが、カートリッジ内の記録媒体のデータに認証を受けていないアクセスがあった場合に、そのアクセスを阻止することはできない。

【０００７】本願出願人により出願され、審査中の米国特許出願（代理人整理番号７２２９／５３１７６）は、記録媒体用のカートリッジに収納され、データ記録容量を監視する監視装置を開示している。この装置は、カートリッジに収納されたコントローラと、カートリッジの側面に配設された接点とを備える。この接点は、ディスクドライブ内の接点に接続され、これによりコンピュータはコントローラにアクセスして、ディスクの状態に関する情報を更新することができる。しかしながら、この装置もユーザがデータにアクセスすることを阻止することはできない。

【０００８】

【発明が解決しようとする課題】上述のように、書き込みができない光ディスクなどの記録媒体に書き込まれたデータは、認証を受けていないユーザのワークステーションにインストールされたり不正にコピーされたりする畏れがある。そのため、製造業者は、ユーザのアクセス又はアクセス回数を制限する必要がある。

【０００９】本発明は、上述の問題に鑑みてなされたものであり、ユーザが記録媒体に記録されたデータやプログラムにアクセスする回数を制限することができるデータ記録装置及びデータ読出方法を提供することを目的とする。

【００１０】さらに、本発明は、カートリッジに収納された書込不可の記録媒体のデータへのアクセスを制限するデータ読出方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上述の課題を解決するために、本発明に係るデータ記録装置は、筐体と、プログラムデータ及び認証要求データを記録し、筐体内に収納された記録媒体と、筐体内に配設され、アクセスデータを記憶する記憶手段と、記憶手段に接続し、該記憶手段と認証情報を送受するインターフェース手段と、記録媒体から認証要求データを読み出し、記憶手段からアクセスデータを読み出して認証情報を確認し、認証信号を生成する認証確認手段と、認証信号を受信するまで記録媒体へのアクセスを阻止するアクセス阻止手段とを備える。

【００１２】また、本発明に係るデータ読出方法は、カートリッジに収納された記録媒体から認証情報を読み出すステップと、カートリッジに配設されたメモリからアクセス情報を読み出すステップと、認証情報とアクセス情報を比較するステップと、アクセスが認証されているときに記録媒体からプログラム情報を読み出すステップとを有する。

【００１３】さらに、本発明に係るデータ読出方法は、製造業者がユーザにパスコードを与えることにより、記録媒体へのアクセス回数を追加する。

【００１４】さらに、本発明に係るデータ記録装置及びデータ読出方法は、書き込みができない記録媒体を収納するカードリッジ内にメモリを設け、ユーザが実際に記録媒体にアクセスした回数をこのメモリに記憶させる。

【００１５】さらに、本発明に係るデータ記録装置及びデータ記録法方は、記録媒体用のドライブに接点を設け、この接点を介して記録媒体を収納するカートリッジ内の装置がドライブと認証情報を交換し、ユーザが記録媒体にアクセスする回数を制限する。

【００１６】本発明のある具体例においては、光ディスクを収納する略方形のカートリッジ内に不揮発性メモリ及びコントローラを設け、これによりユーザが記録媒体にアクセスした回数を計数し、記憶する。また、カートリッジ端部にコントローラに接続された接点を設け、この接点を介して外部のコンピュータがコントローラにアクセスする。コンピュータが光ディスクにアクセスする毎に、アクセス回数に１が加えられる。ユーザの操作により、光ディスクへのアクセスが必要となると、コンピュータはコントローラからアクセスデータを受け取り、このとき所定回数のアクセスが既になされているときは、コンピュータはユーザに対して光ディスクへのアクセスを許可しない。

【００１７】さらに本発明の他の具体例においては、光ディスクドライブに所定数の第１の接点を設け、この第１の接点がディスクカートリッジの側面に設けられた第２の接点に接続すよう構成されたディスクカートリッジ及びディスクドライブを提供する。ディスクコントローラがこれらの接点を介してカートリッジ内のアクセスコントローラに信号を送信し、カートリッジ内にアクセスコントローラが存在するか否かを確認する。このとき、アクセスコントローラが存在すれば、ディスクコントローラはアクセス情報をアクセスコントローラから読み出し、このアクセス情報と光ディスクに記録された認証情報を比較する。これにより、ユーザが認証を受けていることが確認されたとき、アクセスが許可され、アクセスコントローラの認証情報に１を加算する。ユーザが認証を受けていないとき、アクセスを拒否し、光ディスクをディスクドライブから排出する。

【００１８】このように、本発明に係るデータ記録装置及びデータ読出方法は、カートリッジ内に収納された記録媒体へのユーザのアクセス回数を制限し、また認証を受けていないユーザのアクセスを制限する。

【００１９】

【発明の実施の形態】以下、本発明に係るデータ記録装置及びデータ読出方法について、図面を参照しながら詳細に説明する。

【００２０】図１は、本発明の第１の実施の形態である、本発明を適用したディスクカートリッジを示す図である。この図１に示すように、ディスクカートリッジ１は、光ディスク３を収納し、ディスクカートリッジ１の１側面には接点６が設けられている。接点６は、不揮発性のメモリ９を有するアクセスコントローラ８に接続されている。アクセスコントローラ８及びメモリ９の電力はバッテリ１０から供給されている。

【００２１】図２は、ディスクカートリッジ１を収納する光ディスクドライブ２０を示す図である。光ディスク３は、図示しない回転機構により回転駆動され、読出ヘッド２６が光ディスク３に記録されたデータを読み出す。バネ接点２２は、ディスクカートリッジ１の側面に設けられた接点６に対向するように設けられている。バネ接点２２は、アクセスコントローラ８とディスクコントローラ２４を電気的に接続する。このディスクコントローラ２４の他端は、コンピュータ２５に接続されている。読み出しヘッド２６は、このコンピュータ２５に制御されて、光ディスク３からデータ又はプログラムを読み出す。

【００２２】コンピュータ２５は、ディスクコントローラ２４にコマンドを送信し、ディスクカートリッジ１のメモリ９に記憶されているアクセスデータを、アクセスコントローラ８から接点６及びバネ接点２２を介して読み出す。

【００２３】このコンピュータ２５の動作を図３～図５に示すフローチャートを用いて説明する。

【００２４】図３に示すステップＳ１において、ディスクカートリッジ１が光ディスクドライブ２０に挿入される。ステップＳ２において、コンピュータ２５は、ディスクコントローラ２４から供給される信号に基づいて、ディスクカートリッジ１がアクセスコントローラ８を備えているか否かを判定する。

【００２５】ステップＳ２において、コンピュータ２５は、アクセスコントローラ８があると判定したとき、ステップＳ３に進み、光ディスク３から認証情報を読み出す。

【００２６】ステップＳ４において、コンピュータ２５は、ディスク３へのアクセスにはアクセスコントローラ８が必要であるか否かを判定する。アクセスコントローラ８が必要でないとき、コンピュータ２５は、ステップＳ５に進み、ディスク３の通常処理を行う。

【００２７】ステップＳ４において、コンピュータ２５は、光ディスク３に記録されたプログラム又はデータにアクセスするためには、アクセスコントローラ８必要であると判定したとき、ステップＳ６に進み、例えば表示装置などを用いてユーザにアクセス権がないことを通知し、ステップＳ７において、光ディスク３を排出して処理を終了する。

【００２８】ステップＳ２において、コンピュータ２５は、アクセスコントローラ８を検出した場合、ステップＳ８に進む。コンピュータ２５は、アクセスコントローラ８がメモリ９に記憶されている光ディスク３へのアクセス回数Ｎを判定するようにポーリングする。

【００２９】ステップＳ９において、コンピュータ２５は、最大アクセス可能回数Ｍを光ディスク３から読み出す。

【００３０】ステップＳ１０において、コンピュータ２５は、ＮとＭとを比較し、更なるアクセス権がユーザにあるか否かを判定する。ここで、ＮがＭ以下のとき、さらなるアクセス権があり、コンピュータ２５は、ステップＳ１１に進んで、ユーザに残りのアクセス可能回数を知らせる。

【００３１】ステップＳ１２において、コンピュータ２５は、ユーザがディスクカートリッジ１を排出する操作を行ったか否かを判定する。ユーザがディスクカートリッジ１を排出する操作を行わない場合、コンピュータ２５は、ステップＳ１３において通常の処理を行い、以後、ユーザがディスクカートリッジを排出する操作を行うまで、この動作を繰り返す。

【００３２】ステップＳ１２において、ディスク排出コマンドが受信されたとき、コンピュータ２５は、図４に示すステップＳ１４に進む。ステップＳ１４においてコンピュータ２５は、アクセス回数Ｎに１を加え、ステップＳ１５においてディスクカートリッジ１を排出する。

【００３３】図３に示すステップＳ１０において、コン

ピュータ２５は、アクセス回数Ｎが最大アクセス可能回数Ｍを越えていると判定したとき、図５に示すステップＳ１６に進み、光ディスク３へのアクセス権が既になくなっていることをユーザに知らせる。ステップＳ１７において、ユーザは、必要な認証パスコードを例えばコンピュータ２５の備えるキーボード等の入力装置を介してコンピュータ２５に入力し、アクセス回数Ｎをリセットすることができる。この認証パスコードについては後述する。

【００３４】ステップＳ１８において、コンピュータ２５は、入力された認証パスコードが正しいか否かを判定する。認証パスコードが正しいとき、ステップＳ１９において、コンピュータ２５は、メモリ９に記憶されたアクセス回数Ｎを０にリセットしステップ図３に示すＳ１１に進む。

【００３５】図５に示すステップＳ１８において、入力された認証パスコードが正しくないと判定されたとき、コンピュータ２５は、ユーザに対して、光ディスク３の製造元に連絡して正規の認証パスコードを入手するように勧告し、ステップＳ２１においてディスクカートリッジ１を排出する。

【００３６】このディスクカートリッジ１により、例えばコンピュータプログラムをワークステーションにインストールする際に、インストールするワークステーションの数を限定することができる。ユーザはいわゆる機器設定ライセンス（site license）を購入して、このようなディスクカートリッジを受け取り、そこに記録されているプログラムのインストールを所定回数だけ行うことができる。すなわち、ユーザがインストールを行う毎にアクセス回数が増加し、この機器設定ライセンスで許可された最大アクセス回数に達するまで、ユーザはインストールを行うことができる。ここで、ユーザが、このプログラムをさらに別のワークステーションにインストールしようとするとき、ユーザはさらに追加契約を行い、これにより認証パスコードを得て、この認証パスコードを用いてアクセス回数をリセットし、さらに許可された所定回数のインストールを行うことができる。

【００３７】また、この実施の形態において、光ディスク３にビデオデータを記録し、レンタルビデオ店におけるビデオディスクの貸出しに用いることもできる。この場合レンタルビデオ店が、再生回数が限定されたビデオプログラムを購入する。レンタルビデオ店の顧客が支払うレンタル料金は、顧客がビデオを再生した回数に基づいて算出できる。

【００３８】また、本発明の他の実施の形態では、メモリ９に、光ディスク３へのアクセス回数ではなく、光ディスク３のシリアル番号を暗号化して記憶しておくようにしてもよい。すなわち、光ディスク３の製造工程において、光ディスク３には、固有のシリアル番号が割り当てられ、このシリアル番号を暗号化してメモリ９に記憶させる。ディスクカートリッジ１が光ディスクドライブ２０に挿入されると、コンピュータ２５は、光ディスク３のシリアル番号と、メモリ９に記憶されている暗号化されたシリアル番号を比較する。ここで比較された番号が一致しないとき、コンピュータ２５は、光ディスク３が認証されていない複製であるとみなして、ディスクドライブ２０からディスクカートリッジ１を排出する。

【００３９】さらに、このディスクカートリッジ１により、例えば光ディスク３に記録されたオペレーションシステムが特定のコンピュータ２５と一緒に出荷されるような場合に、このオペレーションシステムが他のコンピュータにインストールされることを防止することができる。すなわち、コンピュータ２５の製造業者は、ディスクカートリッジ１内の光ディスク３にオペレーションシステムを記録し、製造した各コンピュータにそれぞれ固有のシリアルナンバーを割り当てる。そして、特定のコンピュータ２５と共に出荷されるディスクカートリッジ１のメモリ９にそのコンピュータ２５のシリアル番号を記憶しておく。このオペレーションシステムは、ディスクカートリッジ１の備えるメモリ９に記憶されているシリアルナンバーがコンピュータ２５のシリアルナンバーに一致する場合にのみ機能するように設計されている。これにより、このオペレーションシステムは、認証されていないコンピュータにインストールして使用することはできない。

【００４０】図６は、従来のディスクドライブ２８に挿入されたディスクカートリッジ１を示す図である。ディスクカートリッジ１のサイズ及び形状は従来のディスクカートリッジに等しい。従来のディスクドライブ２８は、バネ接点を備えておらず、このためコンピュータ２５は、メモリ９に記憶されている情報にアクセスすることができない。光ディスク３に記録されたソフトウェアは、メモリ９に記憶された認証情報にアクセスがなくても、ソフトウェアの一部、例えばデモンストレーション用の一部の機能にアクセスできるように設計されている。このソフトウェアの全機能を使用する為には、ユーザは、本発明を適用したディスクカートリッジに対応するディスクドライブ２０を入手しなくてはならない。

【００４１】図７～図１０は、本発明の第２の実施の形態を示す図である。図７に示すディスクカートリッジ３０は、従来のディスクカートリッジの角部３１を剥離線３３に沿って取り外し可能にしたものである。

【００４２】図８は、ディスクカートリッジ３０から角部３１を取り去り、これに代わるアクセスコントロールモジュール３５をディスクカートリッジ３０と共に示す図である。ディスクカートリッジ３０の突部３８とアクセスコントロールモジュール３５の凹部３９とが係合し、これによりアクセスコントロールモジュール３５は、図９に示すように、ディスクカートリッジ３０に安定的に保持される。

【００４３】図１０は、アクセスコントロールモジュール３５を詳細に示す拡大図である。このアクセスコントロールモジュール３５は、第１の実施の形態におけるディスクカートリッジ１と同様に、アクセスコントローラ８と、メモリ９と、バッテリ１０と、接点６とを備えている。

【００４４】本発明に係るデータ記録装置の第３の実施の形態を図１１に示す。ディスクカートリッジ４０は、側面に接点４１を備え、これら接点４１は、ディスクカートリッジ４０の筐体内に配設されている電気消去可能プログラマブル読出専用メモリ（以下、ＥＥＰＲＯＭという。）４２に電気的に接続されている。このディスクカートリッジ４０は、図２に示す光ディスクドライブ２０に挿入される。ＥＥＰＲＯＭ４２に対しては、第１の実施の形態で説明したようなデータが書き込まれ又読み出されるとともに、ＥＥＰＲＯＭ４２のデータの消去や更新を行う信号も、ディスクコントローラ２４から接点４１を介してＥＥＰＲＯＭ４２に供給される。この実施の形態では、ディスクコントローラ２４から電力及び制御信号がディスクカートリッジ４０に供給されるため、ディスクカートリッジ４０は、第１の実施の形態で説明したディスクカートリッジ１が備えるようなアクセスコントローラ８や、バッテリ１０を必要としない。

【００４５】また、ＥＥＰＲＯＭに代えて、例えばフラッシュメモリ等の不揮発性メモリを持ちいてアクセス情報を記憶するようにしてもよい。

【００４６】上述した実施の形態は、本発明の実施の形態の例示に過ぎず、本発明は、上述した実施の形態の細部により限定されるものではない。当業者は、これらの実施の形態を様々に変形することができるが、それらの変形は、添付の特許請求範囲に記載した本発明の思想に包含されるものである。

【００４７】

【発明の効果】上述のように、本発明に係るデータ記録装置は、筐体と、プログラムデータ及び認証要求データを記録し、筐体内に収納された記録媒体と、筐体内に配設され、アクセスデータを記憶する記憶手段と、記憶手段に接続し、該記憶手段と認証情報を送受するインターフェース手段と、記録媒体から認証要求データを読み出し、記憶手段からアクセスデータを読み出して認証情報＊を確認し、認証信号を生成する認証確認手段と、認証信号を受信するまで記録媒体へのアクセスを阻止するアクセス阻止手段とを備える。

【００４８】また、本発明に係るデータ読出方法は、カートリッジに収納された記録媒体から認証情報を読み出すステップと、カートリッジに配設されたメモリからアクセス情報を読み出すステップと、認証情報とアクセス情報を比較するステップと、アクセスが認証されているときに記録媒体からプログラム情報を読み出すステップとを有する。

【００４９】本発明により、カートリッジの製造業者は、光ディスクなどの読出専用の記録媒体に記録されたデータへのユーザのアクセス又はアクセス回数を制限することができ、認証されていないユーザがデータを使用したり、契約されていないワークステーションにプログラムがインストールされることを防止することができる。

【図面の簡単な説明】

【図１】本発明を適用したディスクカートリッジを示す図である。

【図２】ディスクカートリッジを挿入してデータを読み出すディスクドライブを示す図である。

【図３】データ読み出し動作を説明するフローチャートである。

【図４】図３に示すフローチャートの続きである。

【図５】図３に示すフローチャートの続きである。

【図６】本発明を適用したディスクカートリッジが挿入された従来のディスクドライブを示す図である。

【図７】従来のディスクカートリッジのコーナに剥離線を設けて示す図である。

【図８】コーナが剥離されたディスクカートリッジをアクセスコントロールモジュールとともに示す図である。

【図９】アクセスコントロールモジュールが装着されたディスクカートリッジを示す図である。

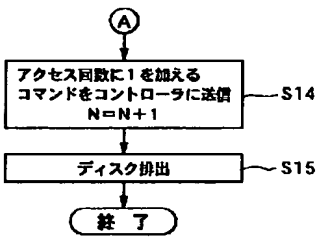
【図１０】アクセスコントロールモジュールの拡大図である。

【図１１】本発明の他の実施の形態を示す図である。

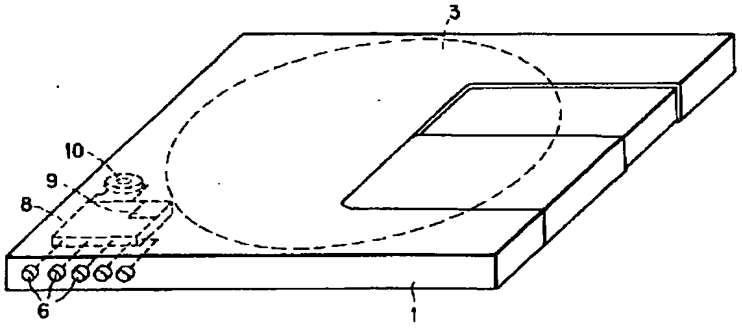
【符号の説明】

１　ディスクカートリッジ、３　記録媒体、６　接点、８アクセスコントローラ、９　メモリ、１０　バッテリ

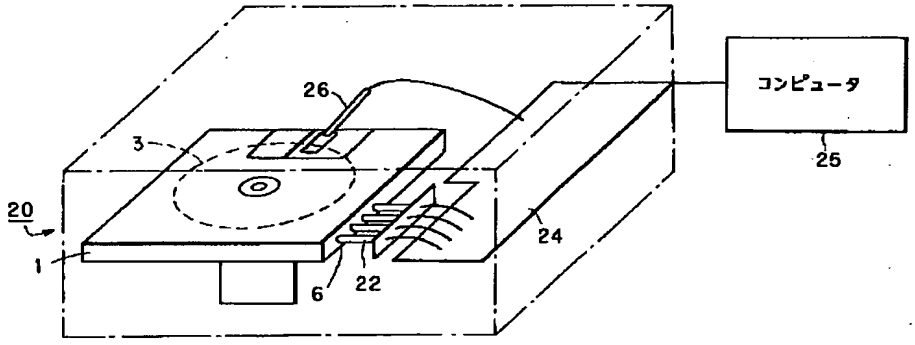
【図４】



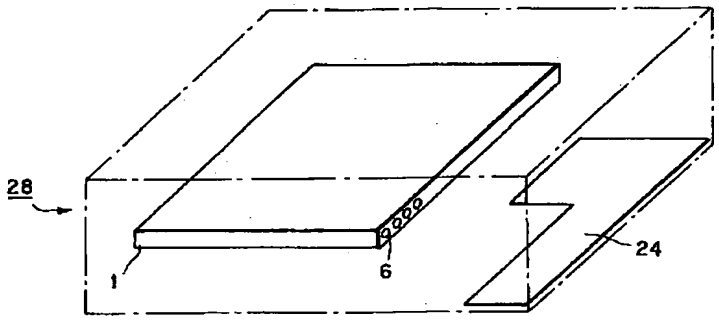
【図１】



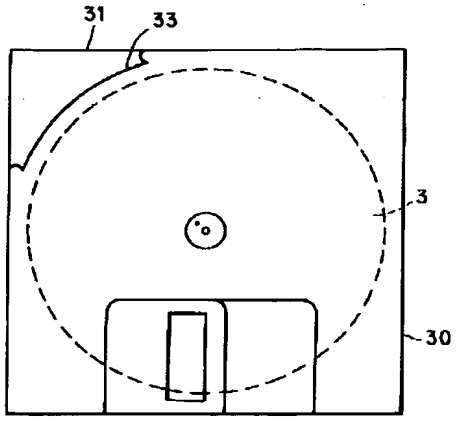
【図２】



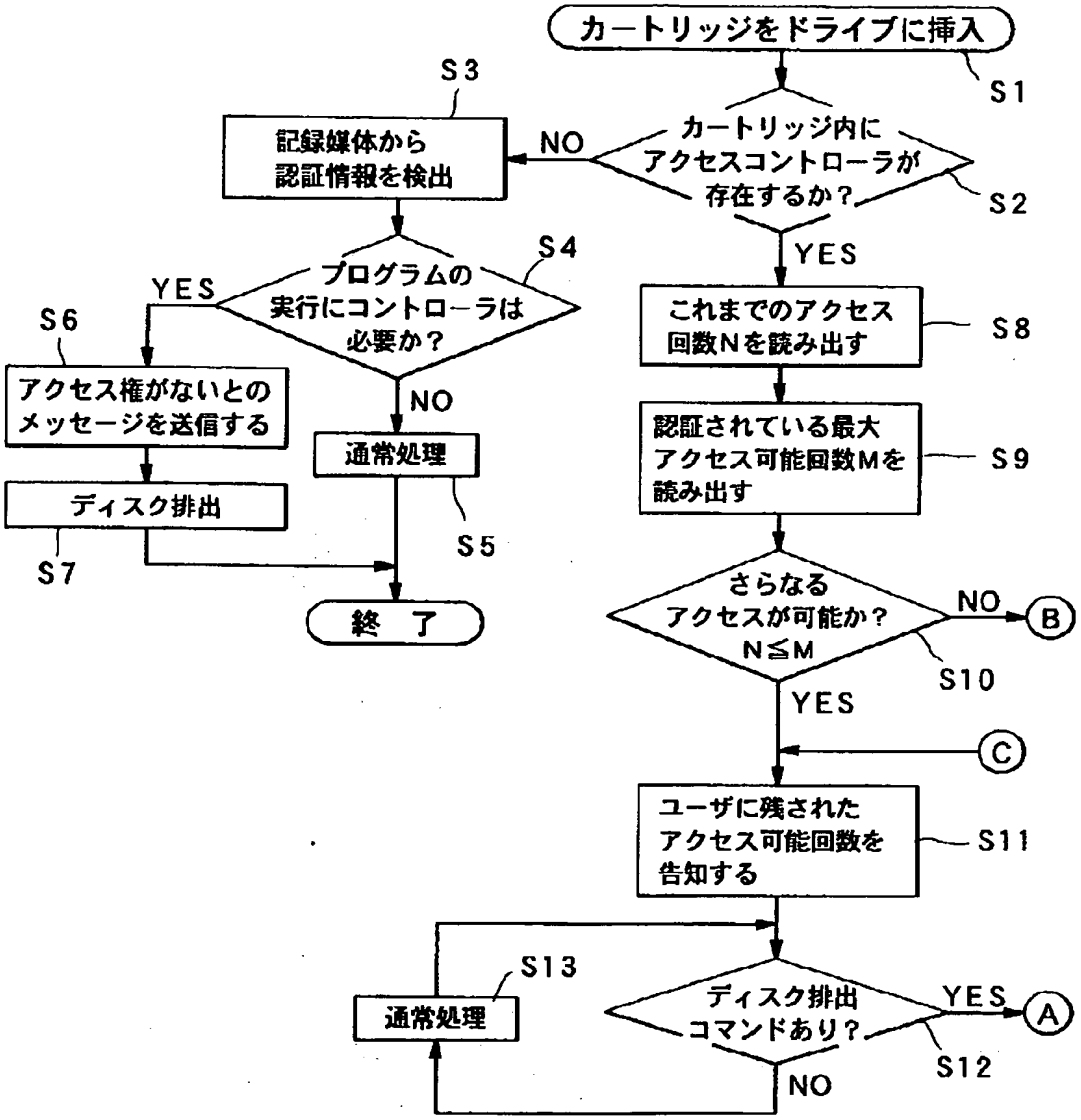
【図６】



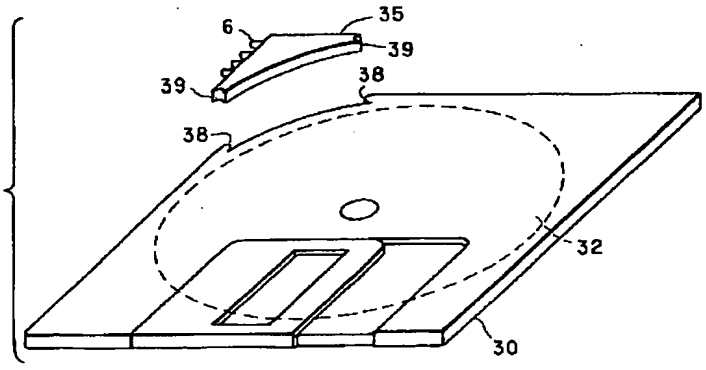
【図７】



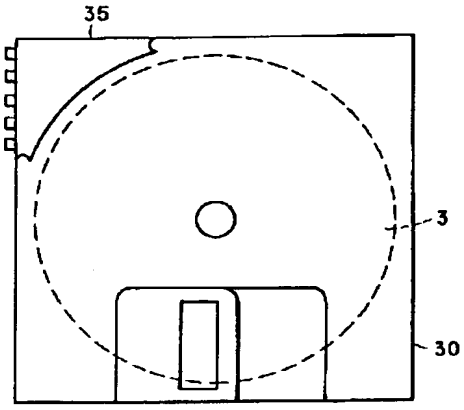
【図３】


カートリッジをドライブに挿入
S1
カートリッジ内にアクセスコントローラが存在するか？
S2
NO
YES
記録媒体から認証情報を検出
S3
プログラムの実行にコントローラは必要か？
S4
YES
NO
アクセス権がないとのメッセージを送信する
S6
ディスク排出
S7
通常処理
S5
終　了
これまでのアクセス回数Nを読み出す
S8
認証されている最大アクセス可能回数Mを読み出す
S9
さらなるアクセスが可能か？ N≦M
S10
NO
B
YES
C
ユーザに残されたアクセス可能回数を告知する
S11
ディスク排出コマンドあり？
S12
YES
A
NO
通常処理
S13

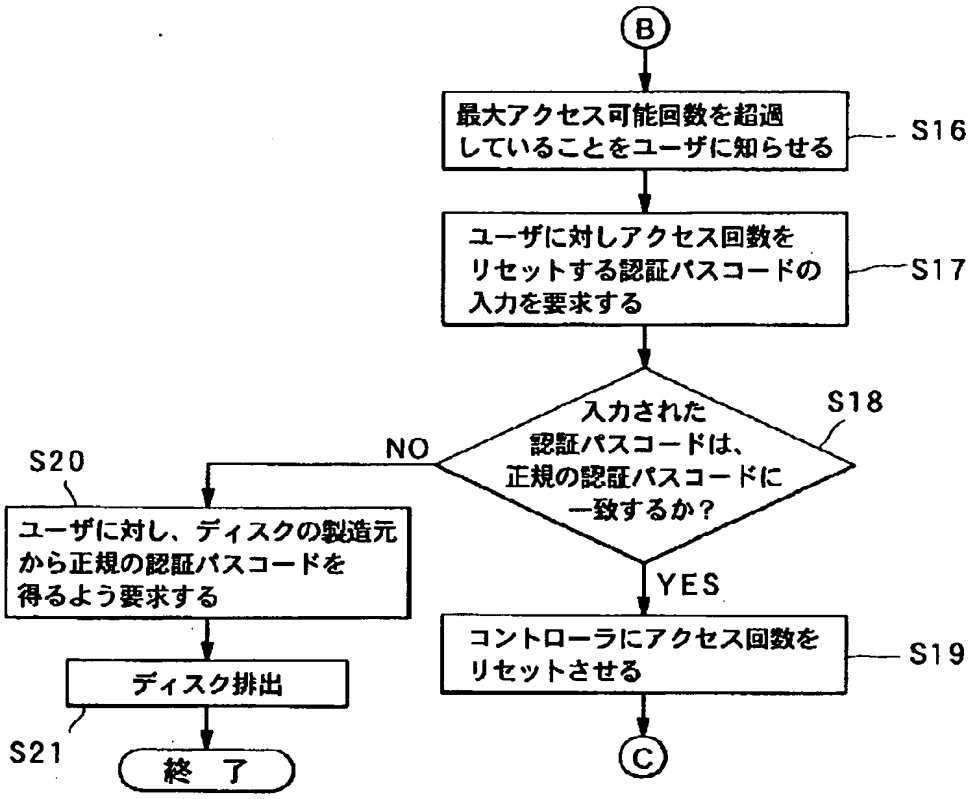
【図８】


6
35
39
39
38
38
32
30

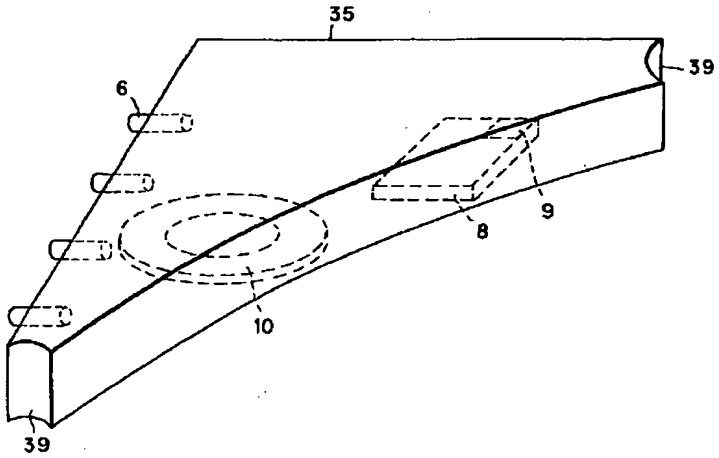
【図９】


35
3
30

【図５】


B
最大アクセス可能回数を超過
していることをユーザに知らせる
S16
ユーザに対しアクセス回数を
リセットする認証パスコードの
入力を要求する
S17
入力された
認証パスコードは、
正規の認証パスコードに
一致するか？
S18
NO
YES
S20
ユーザに対し、ディスクの製造元
から正規の認証パスコードを
得るよう要求する
ディスク排出
S21
終　了
コントローラにアクセス回数を
リセットさせる
S19
C

【図１０】


35
39
6
9
8
10
39

【図１１】